AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1   1. (Currently amended) A method to facilitate locking an adversary out of

2   a network application, comprising:

3   receiving at a server a request, including an authentication credential, to

4   access the network application, wherein the authentication credential includes a

5   user identifier ~~associated with a user~~ and a specific network address of a user

6   device;

7   ~~examining an audit log to determine if the user identifier has been locked~~

8   ~~out from the specific network address; and~~

9   if the user identifier has been locked out from the specific network

10   address,

11   _denying access to the network application; and

12   ~~otherwise, checking the authentication credential for validity, and~~

13   if the authentication credential is valid,

14   allowing access to the network application,

15   otherwise,

16   logging a failed attempt in the audit log,

17   imposing a lockout for the user identifier from only the

18   specific network address after a threshold number of failed

19   attempts from the specific network address,

20   if a threshold number of specific network addresses are

21   locked out for the user identifier, imposing a global lockout for the

22   user identifier, and

23   denying access to the network application;

24   ~~whereby the adversary is prevented from accomplishing an~~

25   ~~attack by masquerading as the user.~~

1   2 (Canceled).

1   3. (Previously presented) The method of claim 1, further comprising:

2   removing a lockout after a predetermined period of time.

1   4. (Previously presented) The method of claim 1, further comprising:

2   manually removing a lockout by an administrator of the server.

1   5. (Original) The method of claim 1, wherein the authentication credential

2   includes a user name and a password.

1   6. (Original) The method of claim 5, wherein checking the authentication

2   credential for validity involves:

3   verifying that an administrator has authorized access to the network

4   application for a combination of the user name and the password; and

5   determining if the request violates an access rule in a rule table.

1   7. (Original) The method of claim 6, wherein the access rule can specify:

2   an allowed time-of-day;

3   an allowed number of access attempts;

4   an allowed network address; and

4

5   an allowed network domain.

1   8. (Original) The method of claim 1, wherein the network address includes

2   an Internet Protocol address.

1   9. (Currently amended) A computer-readable storage medium storing

2   instructions that when executed by a computer cause the computer to perform a

3   method to facilitate locking an adversary out of a network application, the method

4   comprising:

5   receiving at a server a request, including an authentication credential, to

6   access the network application, wherein the authentication credential includes a

7   user identifier ~~associated with a user~~ and a specific network address of a user

8   device;

9   ~~examining an audit log to determine if the user identifier has been locked~~

10   ~~out from the specific network address; and~~

11   if the user identifier has been locked out from the specific network

12   address,

13   denying access to the network application; and

14   ~~otherwise, checking the authentication credential for validity, and~~

15   if the authentication credential is valid,

16   allowing access to the network application,

17   otherwise,

18   logging a failed attempt in the audit log,

19   imposing a lockout for the user identifier from only the

20   specific network address after a threshold number of failed

21   attempts from the specific network address,

22	if a threshold number of network addresses are locked out
23	for the user identifier, imposing a global lockout for the user
24	identifier, and
25	denying access to the network application;
26	~~whereby the adversary is prevented from accomplishing an~~
27	~~attack by masquerading as the user.~~

1   10 (Canceled).

1   11. (Previously presented) The computer-readable storage medium of

2   claim 9, the method further comprising: removing a lockout after a predetermined

3   period of time.

1   12. (Previously presented) The computer-readable storage medium of

2   claim 9, the method further comprising: manually removing a lockout by an

3   administrator of the server.

1   13. (Original) The computer-readable storage medium of claim 9, wherein

2   the authentication credential includes a user name and a password.

1   14. (Original) The computer-readable storage medium of claim 13,

2   wherein checking the authentication credential for validity involves:

3   verifying that an administrator has authorized access to the network

4   application for a combination of the user name and the password; and

5   determining if the request violates an access rule in a rule table.

1   15. (Original) The computer-readable storage medium of claim 14,

2   wherein the access rule can specify:

3   an allowed time-of-day;

4   an allowed number of access attempts;

5   an allowed network address; and

6   an allowed network domain.

1   16. (Original) The computer-readable storage medium of claim 9, wherein

2 the network address includes an Internet Protocol address.

1   17-24 (Canceled).